MEM
F.# 2019R00778

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- X

IN THE MATTER OF AN APPLICATION FOR A SEARCH WARRANT FOR:

THE PREMISE KNOWN AND DESCRIBED AS:

A BLACK SAMSUNG GALAXY NOTE 8, IMEI NUMBER 352590100420672 (THE "SUBJECT TELEPHONE").

- X

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

(Fed. R. Crim. P. 41)

M.J. 19- 603

EASTERN DISTRICT OF NEW YORK, SS:

JUSTIN QUINN, being duly sworn, deposes and states that he is a Special Agent ("SA") assigned to the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), duly appointed according to law and acting as such. Upon information and belief, there is probable cause to believe that there is located in the PREMISES KNOWN AND DESCRIBED AS A BLACK SAMSUNG GALAXY NOTE 8, IMEI NUMBER 352590100420672 (THE "SUBJECT TELEPHONE"), further described in Attachment A, the things described in Attachment B, which constitute evidence, fruits and instrumentalities of a conspiracy to distribute and possess with intent to distribute methamphetamine and the use of a firearm in connection with a Hobbs Act Robbery, in violation of Title 21, United States Code, Sections 841(b)(1)(A)(viii) and 846, and Title 18, United States Code, Section 924(c)(1)(A)(i) and 1951 (the "Target Offenses"), respectively.

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I am a SA assigned to work with the ATF, and have been for more than 12 years. During my tenure with the ATF, I have investigated various federal criminal violations including narcotics trafficking, use of firearms in connection with narcotics trafficking and crimes of violence. During the course of those investigations, I have conducted physical surveillance, monitored undercover operations, debriefed cooperating witnesses and confidential informants, conducted controlled narcotics purchases and interviewed civilian witnesses. The information set forth below is based upon my experience and training as a SA, my review of documents and other evidentiary items, debriefing of cooperating witnesses, and my discussions with other law enforcement agents. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part only. Based on my experience, and in light of the information I have learned during this investigation, I believe there is probable cause that the SUBJECT TELEPHONE was used to communicate with others concerning the Target Offenses, and to receive and store electronic information relating to the names, nicknames, telephone numbers and pager numbers of criminal accomplices. It has been my experience that narcotics traffickers and participants in robberies often communicate by telephone, pager and other electronic devices with their co-conspirators to plan and execute their criminal schemes.

[1] Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

2. The ATF has been conducting an investigation into narcotics trafficking and robberies committed by, or planned to be committed by, CHRISTOPHER KRYSTOFF in Suffolk County, New York and elsewhere.

3. In or about and between April 2019 and June 2019, on at least two separate occasions, an undercover federal agent (the "UC") and/or the cooperating defendant (the "CD") purchased narcotics from KRYSTOFF. In total, law enforcement purchased more than 160 grams of methamphetamine from KRYSTOFF. On each occasion, law enforcement contacted KRYSTOFF by dialing (212) 380-6512, (347) 764-6740, (347) 737-6221 and/or (917) 538-8074. One of these transactions is discussed below.

4. On April 24, 2019, the CD, under the supervision of law enforcement officers, arranged to meet KRYSTOFF at a pre-determined location in Brooklyn, New York. Upon arrival at the location, KRYSTOFF entered the CD's vehicle whereupon they engaged in a discussion. During the course of their conversation KRYSTOFF stated, in sum, substance, and in part, that, "He possessed a firearm, however, he could not sell it to [the CD] because he may need it to commit future robberies." KRYSTOFF further discussed his source of supply for methamphetamine.

5. On May 13, 2019, the UC, arranged to meet KRYSTOFF at a pre-determined location in Hicksville, New York, to purchase methamphetamine by dialing (347) 737-6221. Upon arrival at the location, the UC waited for KRYSTOFF in the UC's vehicle. Within minutes of the UC's arrival, KRYSTOFF arrived at the location, entered the UC's vehicle, and ultimately handed the UC two plastic bags containing a hard crystal substance,

which the UC believed to be methamphetamine. The UC provided KRYSTOFF with $1,200 for the two bags containing the hard crystal substance. KRYSTOFF exited the UC's vehicle and left the location. The substances were subsequently laboratory tested and confirmed to contain cocaine 82.9 grams of pure methamphetamine. This transaction was recorded with both audio and video recording equipment.

6. Based in part on the aforementioned controlled buys, information provided by witnesses and other evidence obtained during the investigation, on or about June 4, 2019, a grand jury sitting in the Eastern District of New York returned an indictment charging KRYSTOFF with conspiracy to distribute and possess with intent to distribute 50 grams or more of methamphetamine and distribution of methamphetamine. See United States v. Christopher Krystoff, 19-CR-252 (DRH). That same day, the Honorable Arlene R. Lindsay, United States Magistrate Judge, signed a warrant authorizing the arrest of KRYSTOFF.

7. On June 4, 2019, the CD arranged to meet KRYSTOFF at a pre-determined location in Hicksville, New York to participate in what KRYSTOFF believed was an armed robbery. Upon arrival at the location the CD parked his/her vehicle. A short time later KRYSTOFF arrived at the location and entered the CD's vehicle. The CD then transported KRYSTOFF to a pre-determined location in Bethpage, New York to meet the UC. Upon arrival at the pre-determined location in Bethpage, KRYSTOFF exited the CD's car and entered the vehicle of the UC, who was parked in his/her vehicle at the location. While inside the UC's vehicle KRYSTOFF stated that in preparation for the robbery he had brought zip ties, a firearm and New York City Police Department ("NYPD") shirts and hats,

to make him appear as if he was a member of law enforcement during the "planned" robbery. KRYSTOFF was arrested at the location and found to be in possession of: (1) one Astra Cadix .38 caliber revolver, serial number 35707; (2) five rounds of .38 caliber Remington ammunition; (3) two NYPD polo shirts; (4) two NYPD reflective vests; (5) an NYPD baseball hat; (6) plastic zip ties; and the SUBJECT TELEPHONE. At the time of his arrest KRYSTOFF had the SUBJECT TELEPHONE on his person.

8. Based on my training, experience and discussions with other law enforcement officers, I understand that individuals involved in the target offenses, often do not act alone and often communicate with co-conspirators by means of cellular telephones such as the SUBJECT TELEPHONE. Such persons commonly maintain records that reflect names, addresses, or telephone numbers of their associates in their cellular telephones. They also commonly maintain records of communications such as call logs, chats and text messages in their cellular telephones. They commonly take photographs of themselves, their associates, or their property using their cellular telephones. These individuals usually maintain these records of communication and photographs in their possession and in their cellular telephones.

TECHNICAL TERMS

9. As used herein, the following terms have the following meanings:

10. Wireless telephone (or mobile or cellular telephone): A handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone

usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving and storing text messages and email; taking, sending, receiving and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device, and a wide variety of applications, also known as "apps," which may store the user's preferences and other data. Such apps may include Facebook, Twitter, and other social media services.

11. Based on my research, I understand that the SUBJECT TELEPHONE provides not only phone and text message services, but can also be used to send and receive emails; access the Internet; track GPS data; take, store and share photographs and videos; and use a wide variety of apps. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the SUBJECT TELEPHONE.

TECHNICAL BACKGROUND

12. As further described in Attachment B, this application seeks permission to locate not only data that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the SUBJECT TELEPHONE was used, the purpose of its use, who used it, and when. There is probable

cause to believe that this forensic electronic evidence can be recovered from the SUBJECT TELEPHONE because:

a. Data on an electronic device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the device that show what tasks and processes were recently active. Web browsers, email programs, and instant messaging/"chat" programs store configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the device was in use. Electronic devices can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, instant messaging or chat logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the electronic device at a relevant time.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw

conclusions about how devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding user attribution evidence, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

13. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for would permit the examination of the SUBJECT TELEPHONE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

14. The ATF seized the SUBJECT TELEPHONE on or about June 4, 2019. Since its seizure, the SUBJECT TELEPHONE has exclusively been in the custody of the

ATF. Additionally, the SUBJECT TELEPHONE is presently in the custody of the ATF in the Eastern District of New York. Because this application seeks only permission to examine the SUBJECT TELEPHONE, which is already in law enforcement's possession, the execution of the warrant does not involve intrusion into a physical location. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

15. Based on the foregoing, there is probable cause to believe that there is located in the SUBJECT TELEPHONE, further described in Attachment A, and the things described in Attachment B, which constitute evidence, fruits and instrumentalities of a conspiracy to distribute and possess with intent to distribute methamphetamine and the use of a firearm in connection with a Hobbs Act Robbery, in violation of Title 21, United States Code, Sections 841(b)(1)(A)(viii) and 846, and Title 18, United States Code, Section 924(c)(1)(A)(i) and 1951. Accordingly, the Court should issue the requested warrant.

16. WHEREFORE, your deponent respectfully requests that a search warrant be issued for the PREMISES KNOWN AND DESCRIBED AS A BLACK SAMSUNG GALAXY NOTE 8, IMEI NUMBER 352590100420672.

Dated: Central Islip, New York
July 1, 2019

JUSTIN QUINN
Special Agent
ATF

Sworn to before me this
1 day of July, 2019

/s/ Gary R. Brown

THE HONORABLE GARY R. BROWN
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

Attachment A

ATTACHMENT A

Property To Be Searched

The property to be searched is a BLACK SAMSUNG GALAXY NOTE 8, IMEI NUMBER 352590100420672 (the "SUBJECT TELEPHONE"); seized on or about June 4, 2019, from the person of CHRISTOPHER KRYSTOFF, who, at the time of the seizure, was standing in Bethpage, New York, and is presently in the custody of the Bureau of Alcohol, Tobacco, Firearms and Explosives in the Eastern District of New York. The warrant authorizes the forensic examination of the SUBJECT TELEPHONE for the purpose of identifying the electronically stored information described in Attachment B.

Attachment B

ATTACHMENT B

Particular Things To Be Seized

All information obtained from the SUBJECT TELEPHONE will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute methamphetamine and the use of a firearm in connection with a Hobbs Act Robbery, in violation of Title 21, United States Code, Sections 841(b)(1)(A)(viii) and 846, and Title 18, United States Code, Section 924(c)(1)(A)(i) and 1951, respectively, including:

1. All records and information on the SUBJECT TELEPHONE described in Attachments A, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) for the time period January 2018 through June 2019, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

2. Evidence of user attribution showing who used or owned the SUBJECT TELEPHONE at the time the things described in this warrant was created, edited, or deleted,

such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control the SUBJECT TELEPHONE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to the SUBJECT TELEPHONE of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT TELEPHONE;

7. Evidence of the times the SUBJECT TELEPHONE was used;

8. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT TELEPHONE; and

9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.